1·P

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,684	08/31/2001	Guy Eden	SLA 1086	2139

55286 7590 06/29/2006

SHARP LABORATORIES OF AMERICA, INC.
C/O LAW OFFICE OF GERALD MALISZEWSKI
P.O. BOX 270829
SAN DIEGO, CA 92198-2829

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/944,684	**Applicant(s)** EDEN, GUY	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14 and 16-27* is/are pending in the application.

4a) Of the above claim(s) *3 and 15* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-14 and 16-27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-2, 4-14, and 16-27 are pending.

Applicant cancels claims 3 and 15.

2. This is a Non-Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4-9, 11-14, and 16-23, 25-27 are rejected under 35 U.S.C. 103(a) as being obvious over Seder, et al. (US 6,401,097).

As per claim 1:

Seder discloses in a digital scanner, a method for secure document transmission the method comprising:

creating computer text files, called profiles, in a directory of a scanner device **(col.2, lines 63-67; the profile in Seder's record is a collection of data**

that is stored in a database), each profile having an address field **(col.3, lines 52-53)** and an encryption field; **(col.6, lines 18-24)**

storing the profiles in a directory; **(col.4, lines 48-53 and 63-65)**

at a scanner device user interface, selecting a profile from the directory; **(col.6, lines 8-12)**

accepting a physical medium document; **(col.5, line 62)**

scanning a document; **(col.5, lines 35-36)**

encrypting the scanned document in response to the encryption field of the selected profile; and, **(col.6, lines 8-13)**

sending the encrypted document to a destination, in response to the address field of the selected profile. **(col.4, lines 28-33 and col.6, lines and 37-58)**

Seder discloses the scanned document to have a watermark **(col.5, lines 33-34)** that identifies the document **(col.4, lines 56-59).** A digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark or can be included in a database record identified by the watermark to help prevent and detect the electronic version of the document from being altered **(col.5, line 62 – col.6, line 4).** Further, Seder discusses that another option is to encrypt an electronic version of a file, an encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark **(col.6, lines 8-13)**. It is obvious that the electronic version of a file is applicant's scanned document because Seder discloses that the encrypted electronic version is identified by the watermark in the database record. Seder did not clearly point out that the encrypted electronic document is a scanned document. In one application, Seder teaches that if watermarks are detected in scan data from an original equipment processing the scanned document data can respond differently**(col.5, lines 30-37).** Thus, it would have been obvious for a person of ordinary skills in the art that the electronic document as taught in Seder has been the scanned document because . the equipment processing in Seder is operable to receive scanned document.

As per claim 2: **See col.4, lines 28-33 and col.6, lines 8-12;** discusses sending the encrypted document to the destination includes sending the encrypted document in response to the address field of the selected profile.

As per claim 3: **Cancelled**

As per claim 4: **See on col.4, lines 35-53;** discusses assigning each profile to a corresponding destination; and, wherein selecting a profile includes: selecting a destination; and, using the profile assigned to the selected destination.

As per claim 5: **See on col.1, lines 61-62;** discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 6: **See on col.6, lines 18-20;** discusses selecting a profile having an encryption field selected from the group including symmetric and asymmetric (public) keys.

As per claim 7: **See on col.6, lines 18-23;** discusses selecting a profile having an asymmetric key; and, wherein creating profiles includes storing public keys in the created profiles.

As per claim 8: **See on col.6, lines 18-20;** discusses selecting a profile having a symmetric key; and, wherein creating profiles includes storing symmetric keys in the created profiles.

As per claim 9: **See on col.4, lines 8-10 and 63-62;** discusses generating a plurality of passwords for the corresponding plurality of user groups; and wherein storing the profiles in a directory includes storing profiles in a profile directory, in response to the generated password.

As per claim 11: See on col.6, lines 18-23; discusses generating a random session key; encrypting the document with the session key using a symmetric algorithm, encrypting the session key with an asymmetric algorithm using the selected profile public key, and wherein sending the encrypted document to the address from the selected profile includes sending the encrypted session key.

As per claim 12: See on col.6, lines 18-23; discusses creating profiles includes creating a profile with a plurality of addresses and a corresponding plurality of public keys, wherein encrypting the document includes generating a single encrypted document using an asymmetric algorithm, and wherein sending the encrypted document includes sending the single encrypted document to each of the plurality of addresses in the profile.

As per claim 13:

Seder discloses in a digital scanner, a method for secure document transmission the method comprising:

storing computer text files, called profiles, in a directory of a scanner device **(col.2, lines 63-67; the profile ii Seder's record which is a collection of data that is stored in a database)**, each profile having an address field **(col.3, lines 52-53)** and an encryption field; **(col.6, lines 18-24)**

at a user interface associated with the scanner device, selecting a profile from the directory; **(col.6, lines 8-12)**

scanning a document; **(col.5, lines 35-36)**

encrypting the scanned document in response to the encryption field of the selected profile; and, **(col.6, lines 8-13)**

sending the encrypted document from the scanner device, to a network-connected destination, in response to the address field of the selected profile. **(col.4, lines 28-37and col.6, lines 18-24 and 37-58)**

Seder discloses the scanned document to have a watermark **(col.5, lines 33-34)** that identifies the document **(col.4, lines 56-59).** A digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark or can be included in a database record identified by the watermark to help prevent and detect the electronic version of the document from being altered **(col.5, line 62 – col.6, line 4).** Further, Seder discusses that another option is to encrypt an electronic version of a file, an encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark **(col.6, lines 8-13)**. It is obvious that the electronic version of a file is applicant's scanned document because Seder discloses that the encrypted electronic version is identified by the watermark in the database record. Seder did not clearly point out that the encrypted electronic document is a scanned document. In one application, Seder teaches that if watermarks are detected in scan data from an original equipment processing the scanned document data can respond differently**(col.5, lines 30-37).** Thus, it would have been obvious for a person of ordinary skills in the art that the electronic document as taught in Seder has been the scanned document because the equipment processing in Seder is operable to receive scanned document.

As per claim 14:

Seder discloses in a digital scanner, a method for secure document transmission the method comprising:

a profile directory having a user interface for selecting computer text files, called profiles **(col.2, lines 63-67; the profile is Seder's record which is a collection of data that is stored in a database)**, each profile including an encryption field **(col.6, lines 18-24)** and an address field; **(col.3, lines 52-53)**

a document scanner to accept physical medium documents , create scanned documents **(col.5, lines 35-36)**, and encrypt the scanned document in response to selected profile encryption fields; and, **(col.6, lines 8-13 and 37-58)**

a network interface for transmitting the encrypted documents to a destination in response to the profile address field. **(col.4, lines 28-33)**

Seder discloses the scanned document to have a watermark where a digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark or can be included in a database record identified by the watermark **(col.5, line 62 – col.6, line 2).** Further, Seder discusses that another option is to encrypt an electronic version of a file, an encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark **(col.6, lines 8-13)**. It is obvious that the electronic version of a file is applicant's scanned document because Seder discloses that the encrypted electronic version is identified by the watermark in the database record. Seder did not clearly point out that the encrypted electronic document is a scanned document. In one application, Seder teaches that if watermarks are detected in scan data from an original equipment processing the scanned document data can respond differently**(col.5, lines 30-37).** Thus, it would have been obvious for a person of ordinary skills in the art that the electronic document as taught in Seder has been the scanned document because [illegible] the equipment processing in Seder is operable to receive scanned document.

As per claim 15: **Cancelled**

As per claim 16: See on col.4, lines 28-33 and col.6, lines 8-12; discusses a memory for storing the profiles; and wherein the profile directory has an interface for creating profiles having an address field and an encryption field.

As per claim 17: See col.1, lines 61-62; discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 18: See col.1, lines 61-62; discusses selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

As per claim 19: **See on col.6, lines 18-23;** discusses the profile directory, and further Seder discusses creating profiles having an address field and an encryption field including symmetric and asymmetric (public) keys.

As per claim 20: **See on col.6, lines 8-23;** discusses the memory stores the public keys corresponding to each profile.

As per claim 21: **See on col.6, lines 18-23;** discusses creating profiles having an address field and an encryption field wherein the memory stores the symmetric keys corresponding to each profile.

As per claim 22: **See on col.4, lines 8-10 and 63-62;** discusses the profile directory, and an interface for generating passwords.

As per claim 24: Seder discusses the document scanner generates a random session key and encrypts the document with the session key using a symmetric algorithm; **(col.6, lines 8-16)** wherein the document scanner encrypts the session key with an asymmetric algorithm using the selected profile public key; and, **(col.6, lines 18-23)** wherein the network interface transmits the encrypted session key with the encrypted document. **(col.6, line 62 – col.6, line 2)**

As per claim 25: Seder the profile directory supplies a selected profile with a plurality of addresses and a corresponding plurality of public keys; **(col.6, lines 22-23)** wherein the document scanner encrypts the document into a single encrypted document using an asymmetric algorithm; and **(col.6, lines 8-10)** wherein the network interface sends the single encrypted document to each of the plurality of addresses in the selected profile. **(col.4, lines 28-33)**

As per claim 26:

Seder discloses a digital scanner secure document transmission system, the system comprising:

a directory **(col.2, lines 63-67; the profile in Seder's record which is a collection of data that is stored in a database)** having a user interface for selecting **(col.6, lines 8-12)** an address field **(col.3, lines 52-53 and col.4, lines 28-37)** cross-referenced to an encryption field; **(col.6, lines 18-24)**

a document scanner to accept physical medium document **(col.5, lines 62)**, create a scanned document **(col.5, lines 35-36)**, and encrypt the scanned document using the cross-referenced generation field; and, **(col.6, lines 8-13 and 37-58)**

a network interface for transmitting the encrypted document to a destination using the selected address field. **(col.5, lines 60-67 col.6, lines 37-58)**

Seder discloses the scanned document to have a watermark **(col.5, lines 33-34)** that identifies the document **(col.4, lines 56-59).** A digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark or can be included in a database record identified by the watermark to help prevent and detect the electronic version of the document from being altered **(col.5, line 62 – col.6, line 4).** Further, Seder discusses that another option is to encrypt an electronic version of a file, an encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark **(col.6, lines 8-13)**. It is obvious that the electronic version of a file is applicant's scanned document because Seder discloses that the encrypted electronic version is identified by the watermark in the database record. Seder did not clearly point out that the encrypted electronic document is a scanned document. In one application, Seder teaches that if watermarks are detected in scan data from an original equipment processing the scanned document data can respond differently**(col.5, lines 30-37).** Thus, it would have been obvious for a person of ordinary skills in the art that the electronic document as taught in Seder has been the scanned document because the equipment processing in Seder is operable to receive scanned document.

As per claim 27:

Seder discloses in a digital scanner, a method for secure document transmission, the method comprising:

cross-referencing an address field **(col.3, lines 52-53)** to an encryption field; **(col.4, lines 56-57)** storing the cross-referenced fields in a directory; **(col.2, lines 63-67; the profile in Seder's record which is a collection of data that is stored in a database)**

at a scanner device user interface, selecting an address from the directory; **(col.4, lines 28-37)**

accepting a physical medium document; **(col.5, lines 62)**

scanning the document; **(col.5, lines 35-36)** encrypting the scanned document using the cross-referenced encryption field; and **(col.6, lines 8-13)**

sending the encrypted document to a destination using the selected address field. **(col.5, lines 60-67 and col.6, lines 18-24 and 37-58)**

Seder discloses the scanned document to have a watermark **(col.5, lines 33-34)** that identifies the document **(col.4, lines 56-59).** A digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark or can be included in a database record identified by the watermark to help prevent and detect the electronic version of the document from being altered **(col.5, line 62 – col.6, line 4).** Further, Seder discusses that another option is to encrypt an electronic version of a file, an encode an encoding key in a watermark in the printed document (or in a database record identified by the watermark **(col.6, lines 8-13)**. It is obvious that the electronic version of a file is applicant's scanned document because Seder discloses that the encrypted electronic version is identified by the watermark in the database record. Seder did not clearly point out that the encrypted electronic document is a scanned document. In one application, Seder teaches that if watermarks are detected in scan data from an original equipment processing the scanned document data can respond differently**(col.5, lines 30-37).** Thus, it would have been obvious for a person of ordinary skills in the art that the electronic document as taught in Seder has been the scanned document because [illegible], the equipment processing in Seder is operable to receive scanned document.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seder, et al., and further in view of Hind, et al. (US 6,980,660).

As per claim 10:

Seder discusses selecting a profile and storing a public key **(col.6, lines 18-23)**; and, wherein encrypting the document using the encryption field **(col.4, lines 56-57)** from the selected profile includes using the public key to encrypt the document. **(col.6, lines 8-13)**

Seder discusses the digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark, or can be included in a database record identified by the watermark (col.5, lines 61-64). However, fails to include the certification authority.

Hind discloses implements security such as authentication and encryption that includes cryptography keys do determine the access privileges (col.7, lines 2-35). Further, Hind uses the Certificate Authority to verify the authenticity of the signature and a public key (col.9, lines 45-53 and col.11, lines 35-38).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to include with the encryption of the document by using the public key as taught by Seder signed by the certification authority as taught by Hind because the Certification Authority verifies the authenticity of the document.

As per claim 23:

Seder discusses a certification authority storing public keys; **(col.8, lines 39-43)**

wherein the network interface for a public key corresponding to the selected profile; and, **(col.6, lines 8-23)** wherein the document scanner uses the public key to encrypt the document. **(col.6, lines 8-13)**

Seder discusses the digital signature generated from an electronic document can be encoded in a printed document as the payload of an embedded watermark, or can be included in a database record identified by the watermark (col.5, lines 61-64). However, fails to include the certification authority.

Hind discloses implements security such as authentication and encryption that includes cryptography keys do determine the access privileges (col.7, lines

2-35). Further, Hind uses the Certificate Authority to verify the authenticity of the signature and a public key (col.9, lines 45-53 and col.11, lines 35-38).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to include with the encryption of the document by using the public key as taught by Seder signed by the certification authority as taught by Hind because the Certification Authority verifies the authenticity of the document.

Response to Arguments

5. **The affidavit filed on 4/6/2006 under 37 CFR 1.131 is sufficient to overcome the Mazzagatte, et al. (US 6,562,583), Koeher (US 6, 188,766), and Weschler, Jr. (US 6,6S1,047) reference.**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100